Gate Fidelities, Quantum Broadcasting, and Assessing Experimental Realization

Hyang-Tag Lim, Young-Sik Ra, Yong-Su Kim, and Yoon-Ho Kim
Department of Physics, Pohang University of Science and Technology (POSTECH), Pohang, 790-784, Korea

Joonwoo Bae*
School of Computational Sciences, Korea Institute for Advanced Study, Seoul, 130-012, Korea
(Dated: June 30, 2011)

We relate gate fidelities of experimentally realized quantum operations to the broadcasting property of their ideal operations, and show that the more parties a given quantum operation can broadcast to, the higher gate fidelities of its experimental realization are in general. This is shown by establishing the correspondence between two operational quantities, quantum state shareability and quantum broadcasting. This suggests that, to assess an experimental realization using gate fidelities, the worst case of realization such as noisy operations should be taken into account and then compared to obtained gate fidelities. In addition, based on the correspondence, we also translate results in quantum state shareability to their counterparts in quantum operations.

PACS numbers: 03.65.Ud, 03.67.Bg, 42.50.Ex

While quantum systems are processed to perform information tasks, building blocks to control and manipulate quantum states of interest are characterized by *positive and completely positive* maps between quantum states. This immediately gives fundamental limitations on quantum state manipulation, and consequently *approximate quantum operations* are naturally followed. Interestingly, approximate operations can be found in important quantum information applications: for instance, approximate quantum cloning implements optimal interaction to learn about given quantum systems [1], or approximate operations to the partial transpose can be used to detect entanglement [2].

This introduces efficient implementation of approximate quantum operations as one of major challenges for quantum information applications, e.g. [3]. As successful realization is closely related to achieving what is aimed by ideal quantum operations, it is thus important how an experimental realization of approximate operations is assessed. Gate fidelities that have been applied to unitary transformations [4] [5], can be extended to general quantum operations since by gate fidelities it is quantified how faithful an experimental realization is. However, we point out that once gate fidelities are computed, interpretation to the obtained values is not clear. For instance, suppose that gate fidelities of experimentally realized operations with respect to the ideal one are obtained about 0.99, which might claim very good performance. But, does it really mean that the ideal quantum operation has been faithfully implemented? As we will show later, what if a complete noise operation such as the depolarization can also achieve about 0.98 in gate fidelities? In fact, gate fidelities can have different ranges according to given quantum operations.

In this work, motivated by the questions addressed in the above, we provide an analysis on and explain ranges that gate fidelities have. Namely, we establish the correspondence between the broadcasting property of quantum operations and gate fidelities of realized operations: the more parties an ideal operation can broadcast to, the higher values gate fidelities of its experimental realizations have in general, regardless of the quality of actual realizations. This is shown by proving that from the isomorphism between states and operations in Ref. [6], *the broadcasting property of quantum operations corresponds to the shareability of quantum states.* We then translate the hierarchy among shareable quantum states into quantum operations, and derive a general lower bound to gate fidelities. This provides both quantitative and qualitative interpretations to gate fidelities: i) by comparing obtained gate fidelities to its lowest bound, an experimental realization can quantified, and ii) using the broadcasting property, obtained gate fidelities can explain how noisier the realization is compared to the ideal one. Through the correspondence, we also translate results in quantum state shareability into properties of quantum broadcasting operations.

Let us begin with identifying gate fidelities that we are going to consider. Throughout the paper, we consider a quantum operation $\mathcal{E}$ which approximates an operation $\mathcal{V}$ that might not be possible in quantum theory. For instance, $\mathcal{E}$ is an optimal quantum cloning that approximates perfect cloning operation $\mathcal{V}$. Let $\mathcal{E}_{\mathrm{ex}}$ denote an experimental realization of the ideal one $\mathcal{E}$. By gate fidelities $\bar{F}$, we mean either the average gate fidelity [4] [5], or the minimum fidelity [7],

$$\bar{F}_{\mathrm{ave}}(\mathcal{E}, \mathcal{E}_{\mathrm{ex}}) = \int d\psi F(\mathcal{E}[\psi], \mathcal{E}_{\mathrm{ex}}[\psi]), \qquad (1)$$

$$\bar{F}_{\mathrm{min}}(\mathcal{E}, \mathcal{E}_{\mathrm{ex}}) = \min_{\psi} F(\mathcal{E}[\psi], \mathcal{E}_{\mathrm{ex}}[\psi]), \qquad (2)$$

*Electronic address: bae.joonwoo@gmail.com

where F denotes Uhlmann's fidelity between quantum states [8]. Gate fidelities in the above estimate the similarity between resulting states by an experimental realization $\mathcal{E}_{\mathrm{ex}}$ and by ideal one $\mathcal{E}$, respectively. We argue that these are appropriate to quantifying experimental realizations $\mathcal{E}_{\mathrm{ex}}$ with respect to the ideal one $\mathcal{E}$. For gate fidelities $\bar{F}(\mathcal{E}, \mathcal{V})$ between $\mathcal{E}$ and $\mathcal{V}$, the meaning is found in the fundamental aspect of quantum operations, i.e. the fundamental limitations in quantum theory to perform an operation $\mathcal{V}$. As an example, perfect cloning $\mathcal{V}$ is approximated by the optimal one-to-two universal quantum cloning $\mathcal{E}$ with fidelity $\bar{F}(\mathcal{E}, \mathcal{V}) = 2/3$ [1]. We emphasize that unless $\mathcal{V}$ can be perfectly done in quantum theory, by gate fidelities $\bar{F}(\mathcal{E}_{\mathrm{ex}}, \mathcal{V})$ neither is shown how successful an experimental realization is, nor the optimality of quantum operations to perform $\mathcal{V}$.

To relate gate fidelities to quantum broadcasting, let us briefly introduce quantum broadcasting and shareability of bipartite quantum states. First, the notion of quantum state shareability reflects the fact that entanglement is a quantum resource that cannot be shared with arbitrarily many parties, also known as monogamy of quantum correlations [9] [10]. To be precise, a bipartite quantum state ρ_{AB_1} is called k-shareable if an extended $k+1$ partite state $\rho_{AB_1\cdots B_k}$ can be found such that bipartite states ρ_{AB_i} for all i are identical, i.e. $\rho_{AB_i} = \rho_{AB_j}$ for $i \neq j$ where $\rho_{AB_i} = \mathrm{tr}_{\bar{A}\bar{B}_i} \rho_{AB_1\cdots B_k}$. This means that when two parties A and B_1 share a k-shareable quantum state, there can exist additional $k-1$ parties such that each of them shares the identical copy with A. This can also be used as an insecurity criteria in quantum key distribution [11]. A remarkable result along the line is that infinitely-shareable quantum states are only separable states [9].

Next, the notion of quantum broadcasting generalizes quantum cloning [12], and has an operational significance in its interpretation: information leaked out during the evolution can be quantified by the number of parties which learn about the resulting state of a given system. By saying that a quantum operation is k-broadcasting, we refer to a positive and completely positive linear transformations from a quantum state to a k-partite state such that quantum states of individual systems are identical. Note that a trace-preserving quantum operation is called a quantum channel. Throughout the paper, we also write $S(\mathcal{H})$ to denote a set of quantum states over Hilbert space $\mathcal{H}$. Then, a quantum channel $\mathcal{E}^{(k)} : S(\mathcal{H}) \to S(\mathcal{H}^{\otimes k})$ is k-broadcasting if for any state $\rho \in S(\mathcal{H})$, the resulting k-partite state, $\rho_{1,\cdots,k} = \mathcal{E}^{(k)}[\rho]$, fulfills that $\rho_i = \rho_j$ for $i \neq j$ where $\rho_i = \mathrm{tr}_{\bar{i}} \rho_{1,\cdots,k}$ [13]. We then write $\mathcal{E}_i^{(k)}$ to denote a local mapping of an ith party as $\mathcal{E}_i^{(k)} : S(\mathcal{H}) \to S(\mathcal{H})$, i.e. $\mathcal{E}_i^{(k)} = \mathrm{tr}_{\bar{i}} \mathcal{E}^{(k)}$.

A quantum operation for a given system corresponds to a local mapping. Once it is implemented, the realization can be completely identified by the so-called quantum process tomography (QPT) [14]. More precisely, a single matrix called the Choi-Jamiolkowski (C-J) state, denoted by $\chi_\mathcal{E} \in S(\mathcal{H} \otimes \mathcal{H})$, is obtained: $\chi_\mathcal{E} = (\mathbb{1} \otimes \mathcal{E})[|\phi^+\rangle\langle\phi^+|]$ where $|\phi^+\rangle = \sum_i |ii\rangle/\sqrt{d}$, and gives the complete characterization of performed operations [6]. Conversely, for a channel $\mathcal{E} : S(\mathcal{H}) \to S(\mathcal{H})$ identified by QPT, one can ask if there could be a k-broadcasting extension $\mathcal{E}^{(k)}$. If an operation $\mathcal{E}$ allows such extension, this means that there can be $k-1$ ancillary systems which can also learn about the resulting state of the system. Quantum operations for which no such extension is possible are, what we call, *private operations* in the sense that the operation does not distribute system's resulting states to any other parties.

Having collected results in the above, we now show the correspondence between quantum broadcasting and quantum state shareability.

A quantum operation $\mathcal{E} : S(\mathcal{H}) \to S(\mathcal{H})$ is a local mapping of a k-broadcasting operation $\mathcal{E}^{(k)} : S(\mathcal{H}) \to S(\mathcal{H}^{\otimes k})$ if and only if its C-J state $\chi_\mathcal{E}$ is k-shareable.

Proof. First, suppose that χ^{AB_1} for an operation $\mathcal{E}_{B_1}$ is $k-$shareable, meaning that there exists an extension $\chi^{AB_1\cdots B_k}$ such that $\chi^{AB_i} = \chi^{AB_j}$ for all i, j. Let us now construct a channel using the extended state, $\mathcal{E}^{(k)} : S(\mathcal{H}) \to S(\mathcal{H}^{\otimes k})$,

$$\mathcal{E}^{(k)}[\rho] = d_A \mathrm{tr}_A[\chi_\mathcal{E}^{AB_1\cdots B_k}(\rho^T \otimes \mathbb{1}_{B_1} \otimes \cdots \otimes \mathbb{1}_{B_k})].$$

Let $\rho_{1,\cdots,k}$ denote a resulting state, $\rho_{1,\cdots,k} = \mathcal{E}^{(k)}[\rho]$, for an input state ρ. Since $\chi^{AB_1\cdots B_k}$ is k-shareable, it holds that $\rho_i = \rho_j$ for all $i \neq j$ and therefore it is shown that $\mathcal{E}^{(k)}$ is k-broadcasting. Then, a local mapping, $\mathcal{E}_i$ of a party B_i for any $i = 1, \cdots, N$ can be found from $\mathrm{tr}_{\bar{i}} \mathcal{E}^{(k)}$, whose C-J state satisfies, $\chi^{AB_i} = \chi^{AB_1}$ for all i.

Conversely, let $\mathcal{E}_i$ denote the ith local mapping of a k-broadcasting channel $\mathcal{E}^{(k)}$, i.e. $\mathcal{E}_i = \mathrm{tr}_{\bar{i}} \mathcal{E}^{(k)}$. All of them are identical, $\mathcal{E}_i[\rho] = \mathcal{E}_j[\rho]$ for all ρ and $i, j \leq k$. This leads to the equality, using the C-J isomorphism, $\mathcal{E}_i[\rho] = d_A \mathrm{tr}_A[\chi^{AB_i}(\rho^T \otimes \mathbb{1})]$, that

$$\chi^{AB_i} = \chi^{AB_j}, \quad \forall i, j \leq k. \tag{3}$$

One can also find a multipartite state from the application of the k-broadcasting channel, $\chi_\mathcal{E}^{AB_1\cdots B_k} = [\mathbb{1} \otimes \mathcal{E}^{(k)}](|\phi^+\rangle\langle\phi^+|)$, in which Eq. (3) holds. This completes the proof that $\chi_\mathcal{E}^{AB_i}$ is k-shareable. $\square$

The result in the above establishes the equivalence between two operational quantities, quantum broadcasting and quantum state shareability, via the isomorphism between quantum states and operations in Ref. [6]. Based on this, results in quantum state shareability can be translated into quantum operations, and vice versa. As an example, let us consider infinitely- and 1-shareable quantum states. Note that C-J states are actually obtained from QPT. That is, *broadcasting properties*

of quantum operations are immediately found from the shareability of C-J states.

First, as it was shown in Ref. [9], only separable states are infinitely-shareable. As separable states correspond to entanglement-breaking channels via the C-J isomorphism [15], *only entanglement-breaking channels can broadcast resulting states to N parties for any N*. This also holds for asymptotic quantum cloning [16], the convergence of which can be found in Ref. [17]. Next, it is clear that pure entangled states are 1-shareable, i.e. for any bipartite entangled state $|\psi\rangle_{AB}$, there is no tripartite state ρ_{ABC} such that $\mathrm{tr}_C\rho_{ABC} = |\psi\rangle_{AB}\langle\psi|$ and $\mathrm{tr}_B\rho_{ABC} = |\psi\rangle_{AC}\langle\psi|$. This means that for a given channel, if its C-J state is pure and entangled, the channel cannot be used for broadcasting of quantum states. Consequently, a unitary transformation can never be used for broadcasting since its C-J state is a maximally entangled state. It is thus shown that *unitary transformations are private operations.*

Proposal to implement private operations. Quantum operations to a given system are generally described by Kraus operators, $\{K_i : K_i^\dagger K_i \geq 0, \quad \sum_i K_i^\dagger K_i = I\}$ such that, $\mathcal{E}[\rho] = \sum_i K_i \rho K_i^\dagger$ [19]. If the evolution is not unitary, its C-J state forms a mixed state allowing an extension to extra parties, and consequently system's resulting states can be broadcasted to a number of parties.

The fact that unitary transformations are private operations can be used to implement approximate quantum operations as private operations. This can be done by applying the Stinespring representation of quantum operations [20]: any quantum operation to a given system can be performed by unitary transformation over given and ancillary systems, i.e. there exist unitary U_{SA} and ancillary state $|a\rangle_A$ such that $\mathcal{E}[\rho_S] = \mathrm{tr}_A U_{SA}\rho_S \otimes |a\rangle_A\langle a|U_{SA}^\dagger$. Since unitaries do not broadcast resulting quantum states, as long as ancillary systems are under control (e.g. stored in quantum memory), no other extra party is allowed to learn about system's resulting states. Therefore, any quantum operation implemented in the Stinespring form is private as long as ancillary systems are under control. This also signifies an operational difference between two alternative descriptions for quantum operations, Stinespring and Kraus forms.

No perfect cloning of unitaries. The fact that unitary transformations cannot be applied for broadcasting of quantum states also leads to a corollary that a unitary transformation cannot be copied. To show this, suppose that perfect cloning of a unitary transformation U is possible. This also means that there exists a C-J state, $\chi_{U\otimes U}$ for two copies of U, such that $\chi_U = \mathrm{tr}_1[\chi_{U\otimes U}] = \mathrm{tr}_2[\chi_{U\otimes U}]$ where tr_i denotes tracing out the ith system. As it was mentioned, however, χ_U is a pure entangled state and does not allow such an extension. This reproduces the result in Ref. [18] that *unknown unitary transformations cannot be perfectly*

cloned. The same also holds true for quantum operations whose C-J states are pure and entangled.

Bounds to gate fidelities. We now derive a general bound to gate fidelities translating the hierarchial structure among shareable quantum states, shown in Ref. [10], into quantum operations. Let S_k denote the set of k-shareable bipartite quantum states. For instance, S_∞ corresponds to separable states and pure entangled states only belong to S_1. A natural relation of inclusion follows, $S_\infty \subset \cdots \subset S_2 \subset S_1$, which has been used to derive a complete criteria for separability of quantum states [10] [21]. The trace distance, defined as $D(\rho,\sigma) = \|\rho - \sigma\|/2$ for states ρ and σ, can be used to estimate distances between quantum states: the minimal distance of a state $\rho \in S_k$ to the set S_∞ is bounded as follows,

$$\min_{\sigma\in S_\infty} D(\rho,\sigma) \leq \epsilon(k), \quad \text{where} \quad \epsilon(1) > \cdots > \epsilon(\infty) = 0. \quad (4)$$

There have also been approaches to derive tighter bounds $\epsilon(k)$ [21], [22].

The hierarchy in quantum state shareability can be translated to quantum operations, via the inequality $F(\rho,\sigma) \geq 1 - D(\rho,\sigma)$ [23]. Recall the relation between quantum operation $\mathcal{E}$ and its C-J state $\chi_\mathcal{E}$, $\mathcal{E}[\rho] = d\mathrm{tr}_A[\chi_\mathcal{E}(\rho^T \otimes I)]$ for a state ρ, where d is the dimension of underlying Hilbert space. From Eq. (4), it follows that for channel $\mathcal{E}$ and an entanglement-breaking one $\mathcal{E}_{EB}$,

$$D(\mathcal{E}[\rho], \mathcal{E}_{EB}[\rho]) \leq dD(\chi_\mathcal{E}, \chi_{\mathcal{E}_{EB}}) \leq d\epsilon(k), \; \forall \rho \in S(\mathcal{H}), (5)$$

where the C-J state $\chi_{\mathcal{E}_{EB}}$ belongs to S_∞. Since D is a distance measure, the triangle inequality holds:

$$D(\mathcal{E}[\rho], \mathcal{N}[\rho]) \leq D(\mathcal{E}[\rho], \mathcal{E}_{EB}^*[\rho]) + D(\mathcal{E}_{EB}^*[\rho], \mathcal{N}[\rho]), \; (6)$$

for some noise channel $\mathcal{N}$, where the channel $\mathcal{E}_{EB}^*$ satisfies: $D(\mathcal{E}[\rho], \mathcal{E}_{EB}^*[\rho]) = \min_{\mathcal{E}_{EB}} D(\mathcal{E}[\rho], \mathcal{E}_{EB}[\rho])$. Note that the noise channel is taken to estimate a worst realization of a given operation $\mathcal{E}$. Applying inequalities Eqs. (5) and (6) in the above, as well as the above-mentioned inequality of fidelity and distance, gate fidelities $\bar{F}(\mathcal{E}, \mathcal{N})$ are bounded as follows,

$$\bar{F}(\mathcal{E}, \mathcal{N}) \geq 1 - d\epsilon(k) - d\bar{D}(\mathcal{E}_{EB}^*, \mathcal{N}), \quad (7)$$

where $\bar{D}$ denotes gate distances, obtained by replacing fidelities in Eqs. (1) and (2) with trace distances.

Therefore, Eq. (7) provides a general lower bound to gate fidelities between a given operation and a noise one. Note that the distance $\bar{D}(\mathcal{E}_{EB}^*, \mathcal{N})$ is generally small since a noise operation is very likely to be entanglement-breaking. Then, the bound depends on the shareability of the C-J state for a given operation, or equivalently, the broadcasting property of a given operation.

From this, we now show that a high value itself in gate fidelities does not suffice to assess experimental realization of quantum operations. Suppose that an approximate operation $\mathcal{E}$, say k-broadcasting, is implemented in
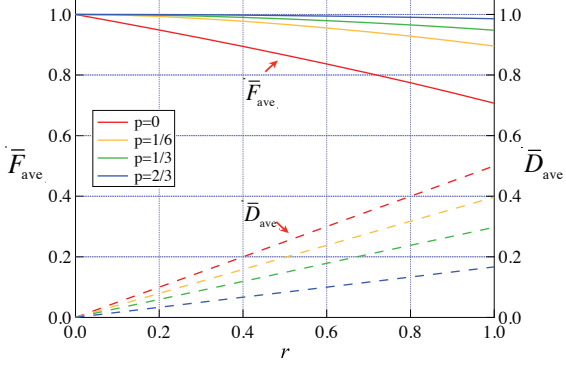
FIG. 1: The average gate fidelity and the average trace distance of the operation in Eq. (8) are shown.

experiment. It follows that $\bar{F}(\mathcal{E},\mathcal{E}_{\mathrm{ex}}) \geq \bar{F}(\mathcal{E},\mathcal{N})$ for a noise operation $\mathcal{N}$. From Eq. (7), no matter how successful or unsuccessful the realization is, gate fidelities are larger than $1 - d\epsilon(k) - d\bar{D}(\mathcal{E}_{EB}^{*},\mathcal{N})$, which is close to $1 - d\epsilon(k)$ since $\bar{D}(\mathcal{E}_{EB}^{*},\mathcal{N}) \ll 1$. That is, we have $\bar{F}(\mathcal{E},\mathcal{E}_{\mathrm{ex}}) \gtrsim 1 - d\epsilon(k)$: *the more parties a given quantum operation can broadcast to, the higher gate fidelities of its experimental realization in general.*

Let us illustrate this with an example, $\mathcal{E}_p[\rho] = (1-p)\rho + \frac{p}{2}(\sigma_x\rho\sigma_x + \sigma_z\rho\sigma_z)$, which is entanglement-breaking for $p \geq 2/3$, and the case with $p = 2/3$ corresponds to an optimal (approximate) transpose operation [24]. Suppose that the operation is realized for a given p under the depolarizing noise,

$$\mathcal{E}_{\mathrm{ex}}[\rho] = (1-r)\mathcal{E}_p[\rho] + r(I/2). \qquad (8)$$

Larger values of r imply more noise in realization. We compute $\bar{F}(\mathcal{E}_p,\mathcal{E}_{\mathrm{ex}})$ in terms of the average fidelity, see Fig. 1. For ideal operation $\mathcal{E}_p$ with larger p (i.e. broadcasting to more parties), the gate fidelity has higher values in general. For instance, when the ideal one is $\mathcal{E}_{p=0}$, the lowest value in the fidelity is about 0.70. For $p = 2/3$, no matter how noisy a performed operation is, the gate fidelity is immediately larger than about 0.98.

Conclusions. We have shown that for a given quantum operation, gate fidelities of its experimental realization are closely related to the broadcasting property of the operation. In fact, the broadcasting property gives a lower bound to gate fidelities of an experimental realization, *independent to how successful or unsuccessful the realization is.* This is obtained by establishing the correspondence between two operational quantities, shareability of quantum states and broadcasting by quantum operations. The correspondence also enables us to translate results in quantum state shareability into broadcasting properties of quantum operations.

On the practical side of assessing experimentally realized quantum operations, we have learned that equal values in gate fidelities for different quantum operations cannot lead to the same conclusion. Moreover, high values in gate fidelities themselves cannot conclude successful realization of quantum operations. Nevertheless, as we have argued in the beginning, gate fidelities are appropriate measures in that they quantify how faithful experimental realization is. The results, therefore, suggest that, to assess an experimental realization of a quantum operation, a lowest bound to gate fidelities should also be presented taking into account the worst case of realization such as noisy operations e.g. the depolarization. In fact, gate fidelities provides information on how good an experimental realization is compared to the worst case of the realization, and how noisier it is than the ideal one in terms of the broadcasting property.

———

[1] W.K. Wootters and W.H. Zurek, Nature **299** 802 (1982); D. Dieks, Physics Letters A, **92(6)** 271 (1982); V. Buzek and M. Hillery, Phys. Rev. A **54** 1844 (1996); V. Scarani *et al.*, Rev. Mod. Phys. **77**, 1225 (2005).

[2] P. Horodecki and A. Ekert, Phys. Rev. Lett. **89**, 127902 (2002).

[3] H.-T. Lim *et al.*, arXiv:1104.3039.

[4] M., P., and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).

[5] M. A. Nielsen, Phys. Lett. A, **303**, 249 (2002).

[6] A. Jamiolkowski, Rep. Math. Phys. **3**, 275 (1972); M. Choi, Linear Algebra and Its Applications, 285, (1975).

[7] N. Johnston and D. W. Kribs, arXiv:1102.0948.

[8] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[9] R. F. Werner, Lett. Math. Phys. **17**, 359 (1989).

[10] A. C. Doherty, P. A. Parrilo and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).

[11] T. Moroder, M. Curty, and N. Lutkenhaus, Phys. Rev. A **74**, 052301 (2006).

[12] H. Barnum *et al.*, Phys. Rev. Lett. **76**, 2818 (1996).

[13] Here, $\mathrm{tr}_{\bar{i}}$ denotes the trace over all systems but the i-th one.

[14] I. L. Chuang and M. A. Nielsen, J. Mod. Opt. **44**, 2455 (1997); J. F. Poyatos, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 390 (1997).

[15] M. Horodecki, P. W. Shor, and M. B. Ruskai, Rev. Math. Phys. **15**, 629 (2003).

[16] J. Bae and A. Acín, Phys. Rev. Lett. **97**, 030402 (2006).

[17] G. Chiribella and G. M. D'Ariano, Phys. Rev. Lett. **97**, 250503 (2006).

[18] G. Chiribella and G. M. D'Ariano, P. Perinotti, Phys. Rev. Lett. **101**, 180504 (2008).

[19] K. Kraus, *States, Effects, andOperations*, (Springer-Verlag, Berlin, 1983).

[20] W. F. Stinespring, Proceedings of the American Mathematical Society, 211, (1955).

[21] M. Navascues, M. Owari, and M. B. Plenio, Phys. Rev. Lett. **103**, 160404 (2009).

[22] F. G.S.L. Brandao, M. Christandl, and J. Yard,

arXiv:1010.1750.

[23] C. A. Fuchs and J. van de Graaf, IEEE Trans. Inf. Theory, **45**, 1216, (1999).

[24] V. Buzek, M. Hillery, and R. F. Werner, Phys. Rev. A **60**, 2626(R) (1999); H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).